INTERNET USE POLICY

Rules and Regulations

DESCRIPTOR CODE: GAHC-R **RESCINDS: GAHC / IFBGA**

BOARD APPROVED: 3/5/2012 **PREVIOUSLY APPROVED: 3/23/2009**

INTRODUCTION

The Gulfport School District is pleased to offer to its students, faculty and staff access to the Internet and the District's Wide Area Network in accordance with the terms and conditions of this policy. The goal of the District in providing this service is to promote educational excellence through access to resources, information and the global community. Network resources are for educational purposes and to carry out legitimate business of the District. Reliable operation of the Network is dependent upon responsible conduct of its users.

Purpose

The purpose of this policy is to outline acceptable use of network resources. These rules are in place to protect users and the District. Inappropriate use exposes the District to risks including virus attacks and compromises data, network systems, and services.

Scope

This policy applies to employees, contractors, consultants, temporaries, students and other workers at the District, including personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by the District or and all equipment that is connected to the district's network systems and/or network services including personal devices.

Monitoring

Network systems include, but are not limited to computer equipment, software, operating systems, storage media, network accounts, electronic mail, Internet service, and file transfer protocol, are the property of the District. Therefore, individual files, computers, electronic mail and other resources of the Network are not private and are subject to inspection and/or monitoring by authorized District officials.

System Resources

The Gulfport School District does not represent or warrant that the functions of the Network system will meet specific requirements or that it will be uninterrupted; nor shall the District be liable for any direct or indirect, incidental, or consequential damages (including lost data and information) sustained or incurred in connection with the use, operation or inability to use the Network system or services.

Warranties/Indemnification

The District is not responsible for material or information accessed on the Internet by users and shall not be responsible for the impact or effect of the information on the user. The District specifically disclaims any responsibility for the accuracy or quality of information obtained via the Internet. The District makes no warranties of any kind, either expressed or implied, in connection with its provision of access to and use of its Network and the Internet. It shall not be responsible for any claims, losses, damages, or costs of any kind suffered, directly or indirectly, by any user arising through the use of the Network or Internet under this policy. As this policy is a legal and binding document, use of the network and district computer resources constitutes agreement by each user to comply with the terms set forth in this policy.

REGULATIONS

Safety and Security

1. Authorized users are responsible for the security of their passwords and accounts. Under no conditions should a user provide his/her password to another person or use another person's password nor should users share accounts.
2. Computers, laptops and workstations should be secured by logging-off when the computer will be unattended.
3. Use of the network will be allowed only with District equipment unless written permission is given by Technology Support Services Department.
4. Computers connected to the Network will continuously execute approved virus-scanning software with current virus definitions. Users should allow updates if prompted.
5. Users should not open e-mail attachments received from unknown senders as they may contain viruses or malicious software.
6. Users should immediately report to Technology Support Services any attempt of others to engage in unauthorized activities, inappropriate communication, or prohibited use of the Internet and district resources.
7. Users may not attempt to circumvent filters, user authentication or security of any host, network, or account on the Network or the Internet. Users should not attempt to gain access to or use equipment assigned to another user without their knowledge.
8. Users are never to give any information about the District's network or computer system to unauthorized individuals or groups.

Children's Internet Protection Act (CIPA)

CIPA requires schools and libraries that receive discounts offered by the E-rate program to have an Internet Safety Policy that includes technology protection measures. The technology protection measures must block or filter Internet access to pictures that are obscene, child pornography or harmful to minors. CIPA also requires schools to adopt and enforce a policy to monitor online activities of minors and adopt a policy that addresses access by minors to inappropriate matter on the Internet, safety and security of minors, unauthorized access and other unlawful activities by minors online, unauthorized disclosure, use, and dissemination of personal information regarding minors, and measures restricting minors' access to materials harmful to them.

1. Gulfport School District will educate minors about internet safety, cyberbullying, social media, and appropriate online behavior through the following: library/media center, technology classes, posters/flyers, and/or television announcements. District employees will be informed of internet safety, cyberbullying, social media, and appropriate online behavior during district professional development.
2. Individually identifiable information about minors such as full name, home address, telephone number or other information that may assist unauthorized individuals identify or contact a minor will ***not*** be made available via District, school or teacher web sites.

Family Educational Rights and Privacy Act (FERPA)

1. The District may authorize the release of directory information as defined by the Family Educational Rights and Privacy Act (FERPA), for internal administrative purposes,

approved educational projects, activities, and publications. Parental permission must be obtained prior to the publication of student directory information.

2. Access to student information is limited to authorized parties and will be permitted only in support of district educational goals and objectives. Parties granted access will fall under the auspices and regulations of this policy and may be required to complete and sign an *Oath of Confidentiality*.

Wireless and Mobile Devices

1. All personal mobile devices such as, but not limited to personal laptops, netbooks, tablet pcs, smartphones, and mp3 players, should be used according to district and school rules and at the discretion of the school.
2. It is mandatory that students use the filtered, wireless network of Gulfport School District (where available) to browse the internet for educational and instructional purposes.
3. Student use of any other wireless network is prohibited.
4. Displaying information to students from any unfiltered, wireless network is prohibited.

Unacceptable Use

Under no circumstances is an employee of the District authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing District resources.

Users shall *not* use Network Email or Resources to:

1. Send mass email mailings of any notice that are not related to district business.
2. Forge email headers to obscure the true originator of an email message.
3. Create or participate in pyramid schemes or email chain letters.
4. Post anonymous messages.
5. Read, delete, copy or modify the email or files of other users or deliberately interfere with the ability of other users to send or receive email.
6. Misrepresent other users or use another person's email address, user account or password.
7. Vandalize a computer system and/or damage the data, files, operations, software, or hardware components.
8. Upload, create or attempt to create a computer virus.
9. Use while access privileges are suspended or revoked.
10. Participate in chat rooms or instant messaging without the permission and direct supervision of a teacher or authorized supervisor.
11. Obtain, copy or modify files, passwords, data or information belonging to other users.
12. Improperly restrict or inhibit other users from accessing and using the Network.
13. Encumber disk space, processors, bandwidth or other system resources so as to interfere with normal use of services on the Network or other systems or networks.

Users shall not access, download, install, transmit, retransmit, submit, publish, display, or print:

14. Defamatory, abusive, profane, sexually-oriented, threatening, racially offensive, illegal,

written or visual depictions of obscene material, child pornography and other materials considered harmful or inappropriate.

15. Material that is threatening, disruptive, or that could be construed as harassment or disparagement of others based on their race**,** national origin, sex, sexual orientation, age, disability, religion or political beliefs.
16. Copyrighted materials, software, shareware, freeware, or material protected by trade secret unless user is in possession of a legal license to do so.
17. Material that promotes violence or injury to persons or the destruction of property by devices including, but not limited to, the use of firearms, explosives, fireworks, smoke bombs, incendiary devices, or other similar materials.
18. Material that is libelous, slanderous, gang-related or incites students and/or staff so as to create a clear and present danger of (a) the commission of unlawful acts on school premises, (b) the violation of law and/or administrative regulations, or (c) the substantial disruption of the orderly operation of the District or any school in the District.

Process for Parents/Guardians to Restrict Internet Access

If a parent/guardian does not wish a student to have access to the Internet, that parent/guardian shall send a letter to that effect to the school principal. Copies of all such letters shall be placed in the child's permanent record.

Sanctions

1. Use of the Network and its resources is a privilege, not a right. Violations of the regulations of this policy may result in the denial, revocation, suspension, termination of the user's privileges and/or disciplinary action that may include student expulsion, employee dismissal, and/or notification of appropriate authorities.
2. Vandalism may result in cancellation of privileges and/or disciplinary action. Vandalism includes any malicious attempt to access, damage, delete, infect, destroy or alter data files, folders, or directories.
3. GSD will fully cooperate with local, state, and/or federal officials in any investigation related to illegal activities conducted through use of the District Network, the Internet or any of its resources.

Legal Reference: Children's Internet Protection Act; Family Educational Rights and Privacy Act (20 USC § 1232g)

Internet Use Policy Agreement

I certify that I have read Policy GAHC-R / JCBA-R. I understand and agree to comply with the terms and conditions of the policy. I understand that any violation of this policy may result in temporary or permanent loss of Network and/or Internet access and my user account; may result in disciplinary action; and may constitute a criminal offense. I, the undersigned, agree not to hold the District responsible for and waive any claim for any loss or damage arising as a result of my use of the system and agree to indemnify and hold harmless the District from any loss or claim which may arise as a result of my actions or failure to act in connection with any use of the system.

_____ _____

Signature Date